AD Canaries: Un canari sorti du chapeau

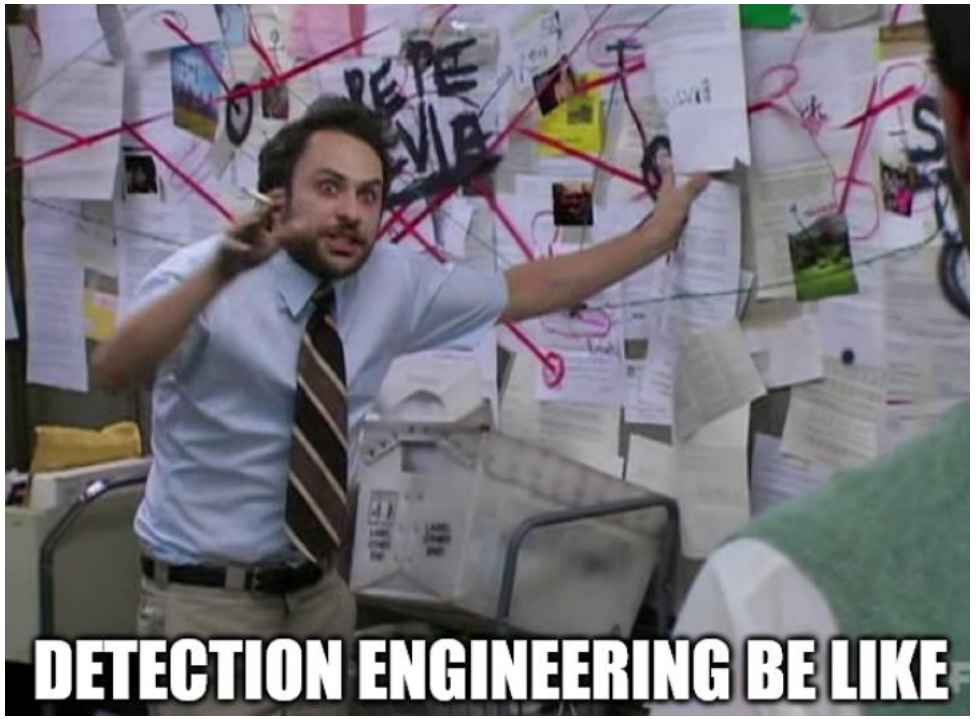
Détournement des DACL backdoors (Specter Ops 2017)
pour permettre une détection efficace de l'énumération Active Directory

Quentin ARNOULD – Analyste SOC

AIRBUS

`whoami` ?

- Quentin Arnould
- SOC Analyst @ Airbus Protect



Ce qui me passionne:

- Analyse d’attaques et la conception de techniques detection
- Sécurité Active Directory
- Analyse d’incidents sur capteurs EDR
- Faire des memes de qualité non contrôlée

AIRBUS

Agenda

- ❑ Enumération Active Directory
- ❑ Opportunités & problématiques de détection
- ❑ DACL Backdoors – An ACE Up the Sleeve, SpecterOps (2017)
- ❑ AD Canaries : mécanisme de détection & résultats en laboratoire
- ❑ AD Canaries : RETEX déploiement en production

AIRBUS

Enumération Active Directory

Etablir un inventaire (exhaustif) des objets Active Directory, présents dans l'environnement

- **Chemin de compromission** (relations de contrôle)
- Faiblesses de configuration
- Ressources critiques
- Elévation de privilèges
- Latéralisation
- …

Outils offensifs « classiques »:

- ❑ PowerSploit
- ❑ BloodHound
- ❑ Pywerview
- ❑ ADFind
- ❑ Rubeus
- ❑ …

Built-ins Windows:

- ❑ Dsget / Dsquery
- ❑ Net.exe / net1.exe
- ❑ Nltest.exe
- ❑ ActiveDirectory Powershell module
- ❑ …

AIRBUS

Enumération Active Directory

https://github.com/infosecn1nja/AD-Attack-Defense

AIRBUS

Enumération Active Directory

x k/m€

Détecter & endiguer l'adversaire

Tempo indicatif - opérateur ransomware observé par notre équipe CSIRT

Détection énumération AD

t_0 5min 24h 36h 38h

Initial intrusion | Persistance, **reconnaissance**, lateral movement | Privilege escalation | Wait for OBH | Defence removal | Cypher all the things

Phishing, vulnerable frontend (VPN…)

Cobalt Strike

Living-of-the-land

Unpatched workstation, admin cleartext

Deactivate / uninstall AV,

Reset / lock admin accounts

You're toast, adversary has been with you a few hours or days

1k€

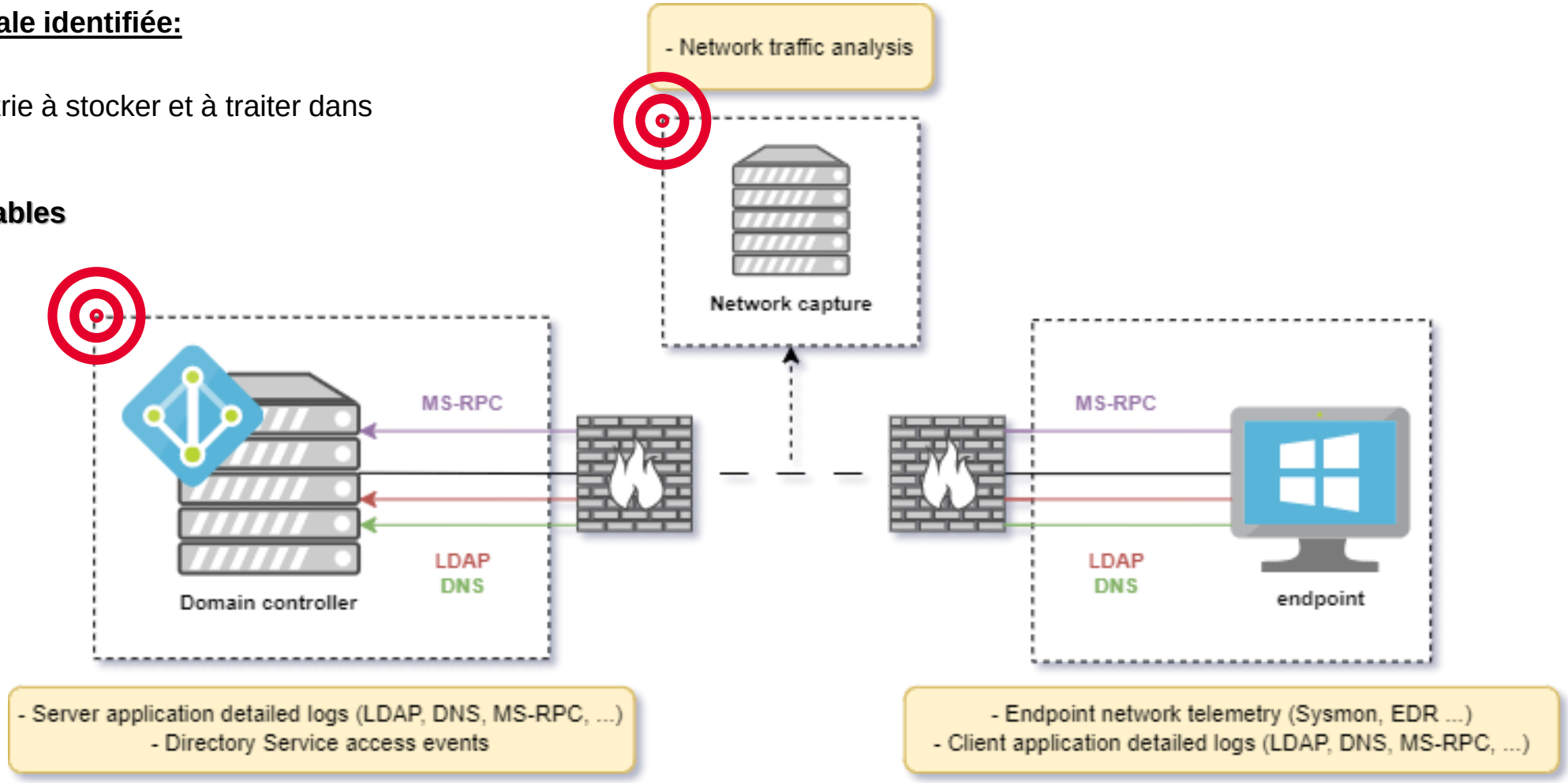
AIRBUS

Opportunités & problématiques de détection

Problématique principale identifiée:

Volumétrie de la télémétrie à stocker et à traiter dans les outils de détection

→ **coûts non négligeables**



AIRBUS

Opportunités & problématiques de détection

Environnement de production ~650 endpoints

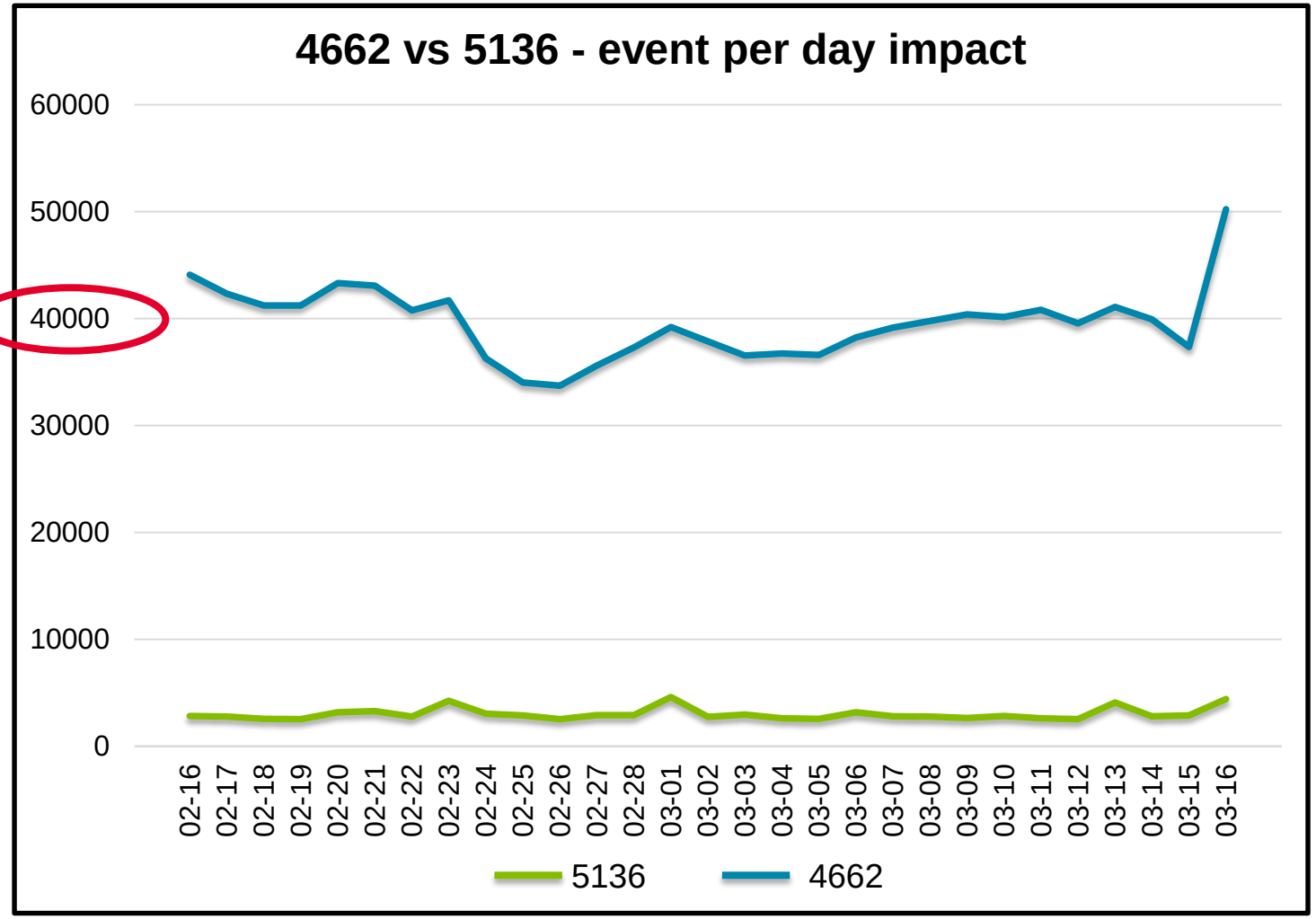
Event 4662 – Directory Service Object Access

Event 5136 – Directory Service Object Modification

Contribuent tous deux à la stratégie de supervision Active Directory

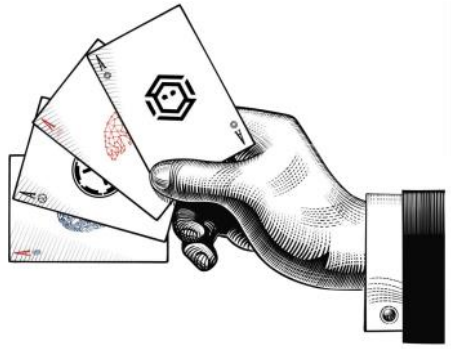
→ Coût volumétrique pour un apport “*similaire*” à la supervision AD

~15 fois plus d’événements 4662 ! (40 000 events/j)



AIRBUS

DACL Backdoors – An ACE Up the Sleeve, SpecterOps (2017)



DACL Backdoor → Active Directory malwareless (privileged) persistence

An ACE Up the Sleeve:

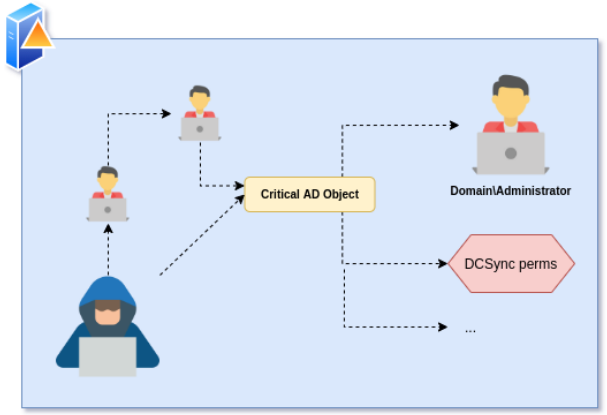
Designing Active Directory DACL Backdoors

Will Schroeder

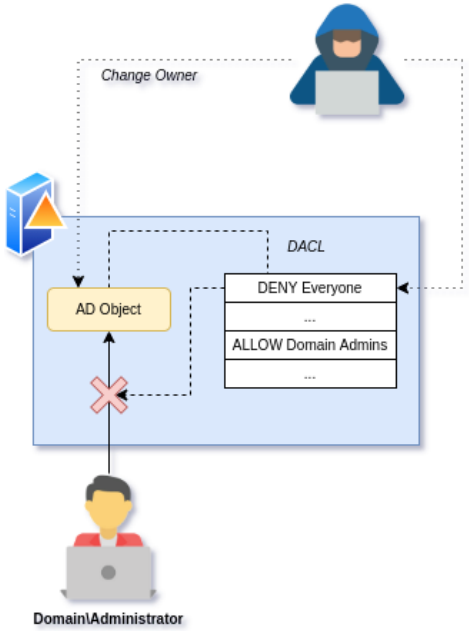
Andy Robbins

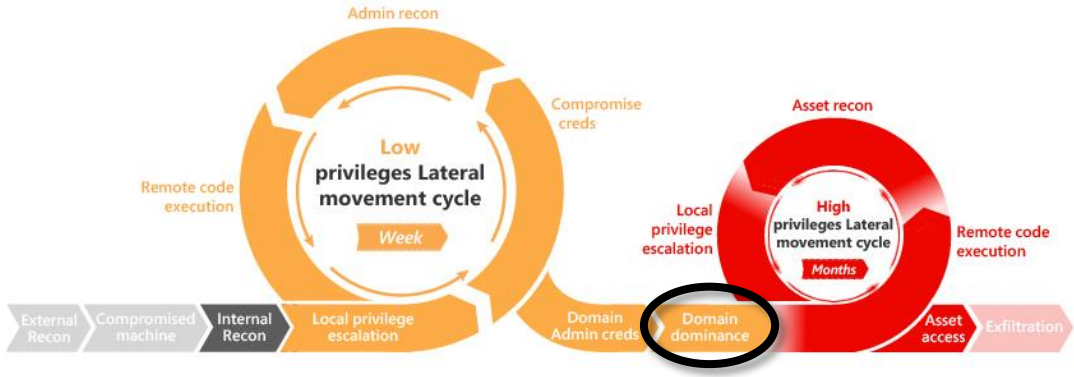
Lee Christensen

Backdoor primitives



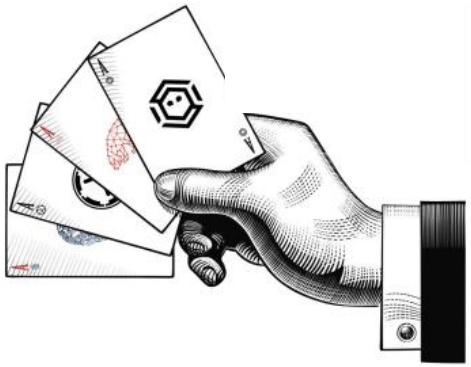
Stealth primitives



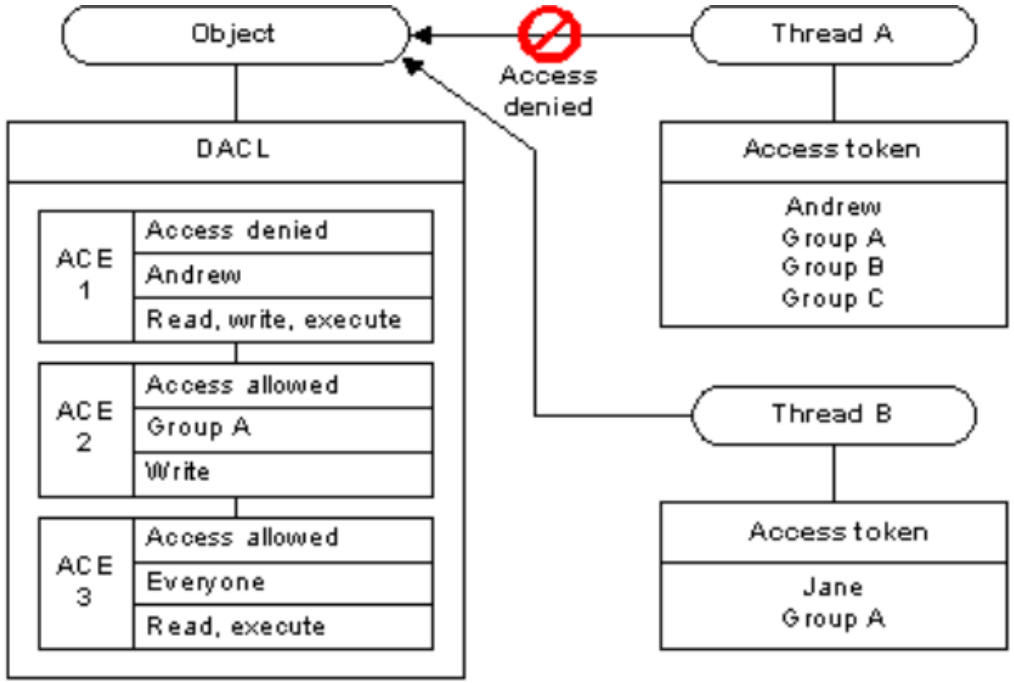


AIRBUS

DACL Backdoors – An ACE Up the Sleeve, SpecterOps (2017)



Discretionary Access Control List – DACL :



https://learn.microsoft.com/en-us/windows/win32/secauthz/dacls-and-aces

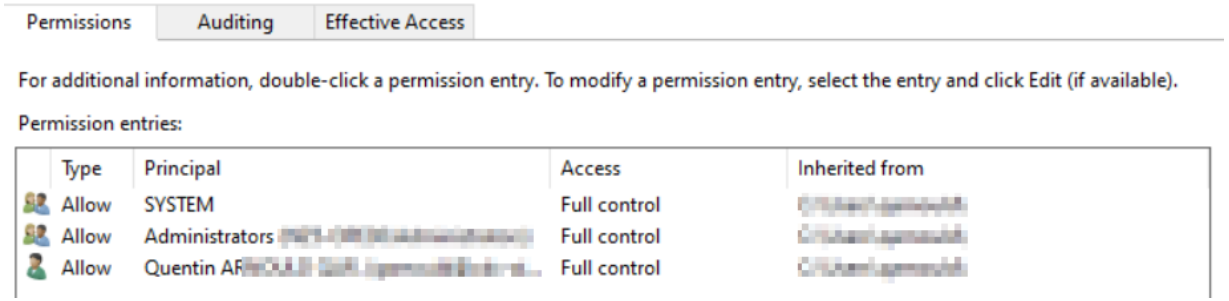
An **ACE** Up the Sleeve:

Designing Active Directory DACL Backdoors

Will Schroeder

Andy Robbins

Lee Christensen



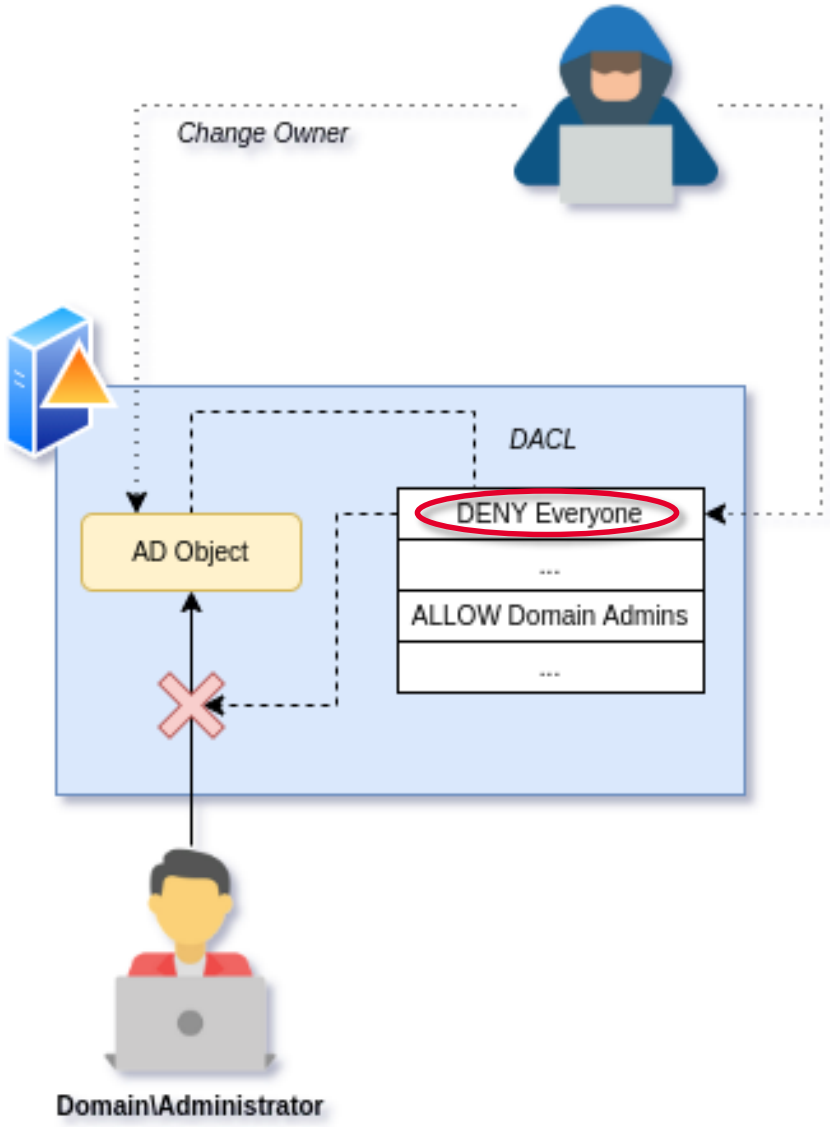
AIRBUS

DACL Backdoors – An ACE Up the Sleeve, SpecterOps (2017)

Stealth Primitives [dissimulation]

- Ordre d'évaluation des DACL :

1. **Explicit DENY**
2. Explicit ALLOW
3. Inherit DENY
4. Inherit ALLOW



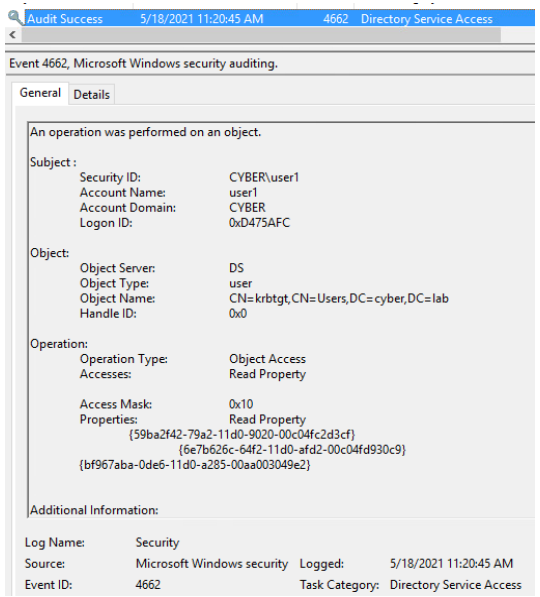
AIRBUS

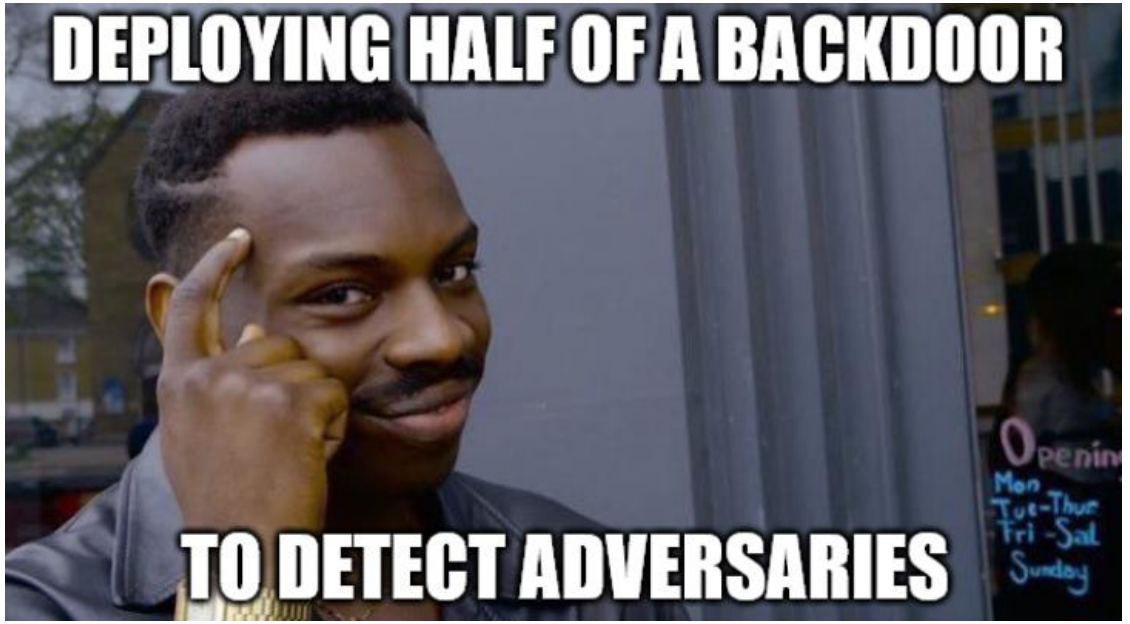
AD Canaries : mécanisme de détection & résultats en laboratoire

Déployer des objets AD qui lorsqu'ils seront accédés (« écrasés ») témoigneront d'une énumération dans Active Directory

- Détournement de la « stealth primitive » des DACL backdoors

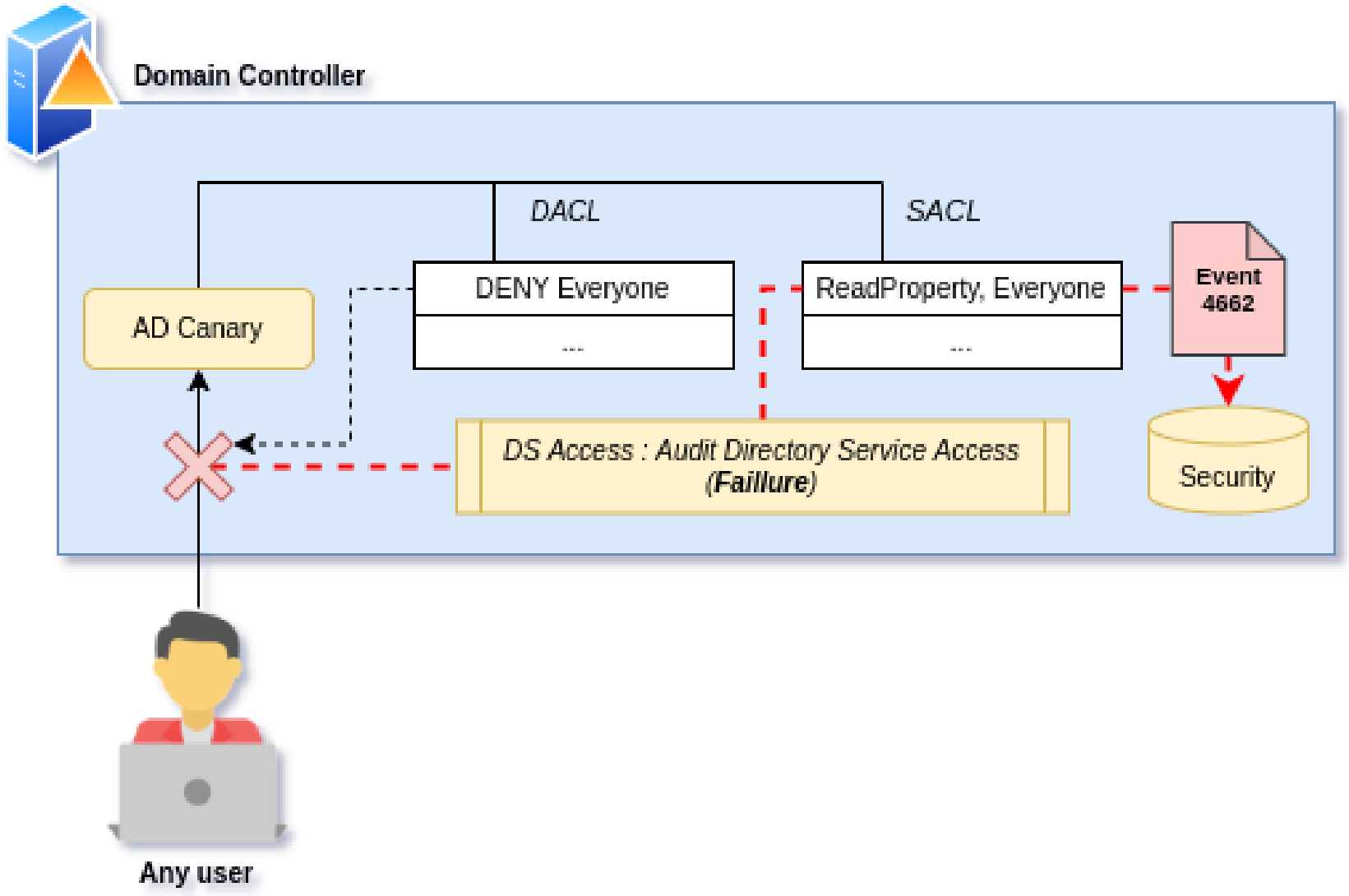
➔ Déployer des objets qui n'ont aucune réalité dans l'environnement
➔ « Cacher » le canari dans l'environnement (Stealth Primitive)
➔ Auditer les tentatives d'accès échoués aux canaris





AIRBUS

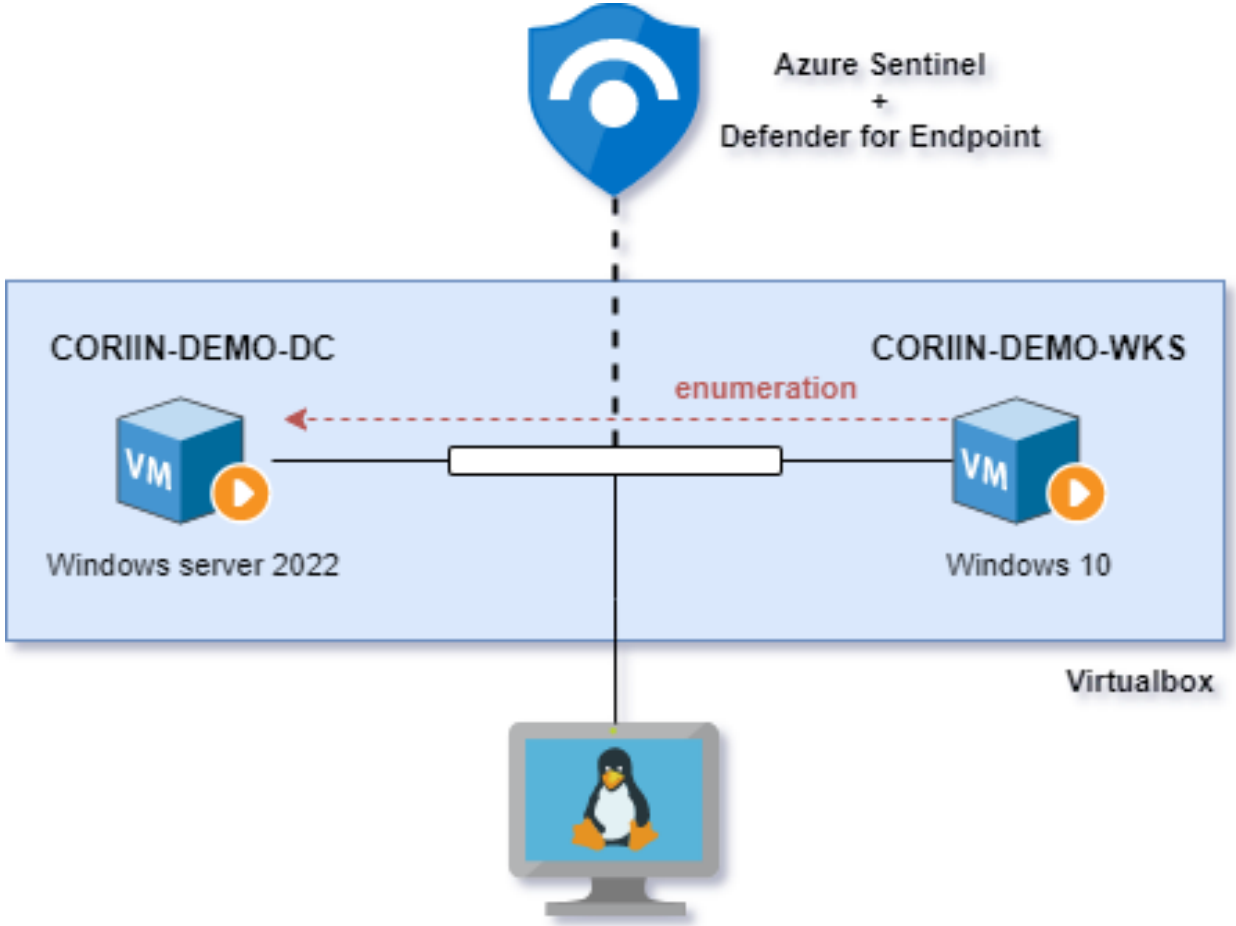
AD Canaries : mécanisme de détection & résultats en laboratoire



AIRBUS

AD Canaries : mécanisme de détection & résultats en laboratoire

Démonstration :



AIRBUS

AD Canaries : mécanisme de détection & résultats en laboratoire

```
SecurityEvent
| where EventID == 4662 and ObjectServer == "DS" and Computer contains "CORIIN"
| extend Object = tostring(split(split(ObjectName, "{")[1], "}")[0]),
         AccessedProperties = extract_all(@"\{([a-fA-F\d]{8}-[a-fA-F\d]{4}-[a-fA-F\d]{4}-[a-fA-F\d]{4}-[a-fA-F\d]{12})\}", Properties)
// ADCanaries.csv generated when deploying via the aforementioned script
| lookup kind=inner _GetWatchlist("ADCanaries") on $left.Object==$right.SearchKey
| mv-expand AccessedProperties
| extend Prop = tostring(AccessedProperties)
// PropertiesGUIDs.csv generated when deploying via the aforementioned script
| lookup kind=leftouter _GetWatchlist("SchemaIDGuids") on $left.Prop==$right.SearchKey
// Simple DIY lookup table using MS documentation for event 4662
| lookup kind=leftouter _GetWatchlist("AccessTypes") on $left.AccessMask==$right.SearchKey
| join kind = leftouter (
    SecurityEvent
    | where EventID == 4624 and LogonType == 3
) on $left.Computer==$right.Computer and $left.SubjectLogonId==$right.TargetLogonId and $left.SubjectUserName==$right.TargetUserName
// Some aggregation here, not optimal
| summarize Count=count(), AccessedProps=makeset(ldapDisplayName), LogonIds=makeset(SubjectLogonId), Accesses=makeset(Access), IPs=makeset(IpAddress1), Devices=makeset(WorkstationName1)
by bin(TimeGenerated, 1m), SubjectUserName, SubjectDomainName, CanaryName, Object
```


AIRBUS

AD Canaries : mécanisme de détection & résultats en laboratoire

Net.exe

Rubeus.exe

ADFind.exe

Results | Chart | Add bookmark

TimeGenerated [UTC]	SubjectUserName	SubjectDomainName	CanaryName	Object	Count	AccessedProps	LogonIds	Accesses	IPs
3/29/2023, 3:19:00.000 PM	Administrator	SYLVESTER	CanaryGroup	b1a40f13-b00e-4...	120	["","objectGUID","name","objectClass"]	["0x6c625"]	["Read Property"]	["10.0.2.12"]
3/29/2023, 3:19:00.000 PM	Administrator	SYLVESTER	CanaryComputer	1a85c65e-7154-4...	120	["","objectGUID","name","objectClass"]	["0x6c625"]	["Read Property"]	["10.0.2.12"]
3/29/2023, 3:19:00.000 PM	Administrator	SYLVESTER	CanaryUser	cf03c42f-eb82-4...	120	["","objectGUID","name","objectClass"]	["0x6c625"]	["Read Property"]	["10.0.2.12"]
3/29/2023, 3:20:00.000 PM	net-enum	SYLVESTER	CanaryGroup	b1a40f13-b00e-4...	3	["","sAMAccountType"]	["0xb5c745"]	["Read Property"]	["10.0.2.151"]
3/29/2023, 3:20:00.000 PM	net-enum	SYLVESTER	CanaryComputer	1a85c65e-7154-4...	3	["","sAMAccountType"]	["0xb5c745"]	["Read Property"]	["10.0.2.151"]
3/29/2023, 3:20:00.000 PM	net-enum	SYLVESTER	CanaryUser	cf03c42f-eb82-4...	3	["","sAMAccountType"]	["0xb5c745"]	["Read Property"]	["10.0.2.151"]
3/29/2023, 3:20:00.000 PM	rubeus	SYLVESTER	CanaryUser	cf03c42f-eb82-4...	13	["","userAccountControl","sAMAccountType","servicePrinci...	["0xb5c81b","0xb5c86c"]	["Read Property"]	["10.0.2.151"]
3/29/2023, 3:20:00.000 PM	adfind-enum	SYLVESTER	CanaryUser	cf03c42f-eb82-4...	3	["","objectCategory"]	["0xb5d56e"]	["Read Property"]	["10.0.2.151"]
3/29/2023, 3:20:00.000 PM	adfind-enum	SYLVESTER	CanaryComputer	1a85c65e-7154-4...	3	["","objectCategory"]	["0xb5d65a"]	["Read Property"]	["10.0.2.151"]

AIRBUS

AD Canaries : mécanisme de détection & résultats en laboratoire

Avantages de cette primitive de détection

- Volumétrie négligeable (cf RETEX)

- Détecte le mécanisme d'énumération AD

- Canaris invisibles pour l'adversaire

  → l'adversaire ne sait pas qu'il est détecté

  → n'impacte pas une posture IR élevée (PRIS)

AD Canaries : RETEX déploiement en production

Environnement de production
~1000 endpoints

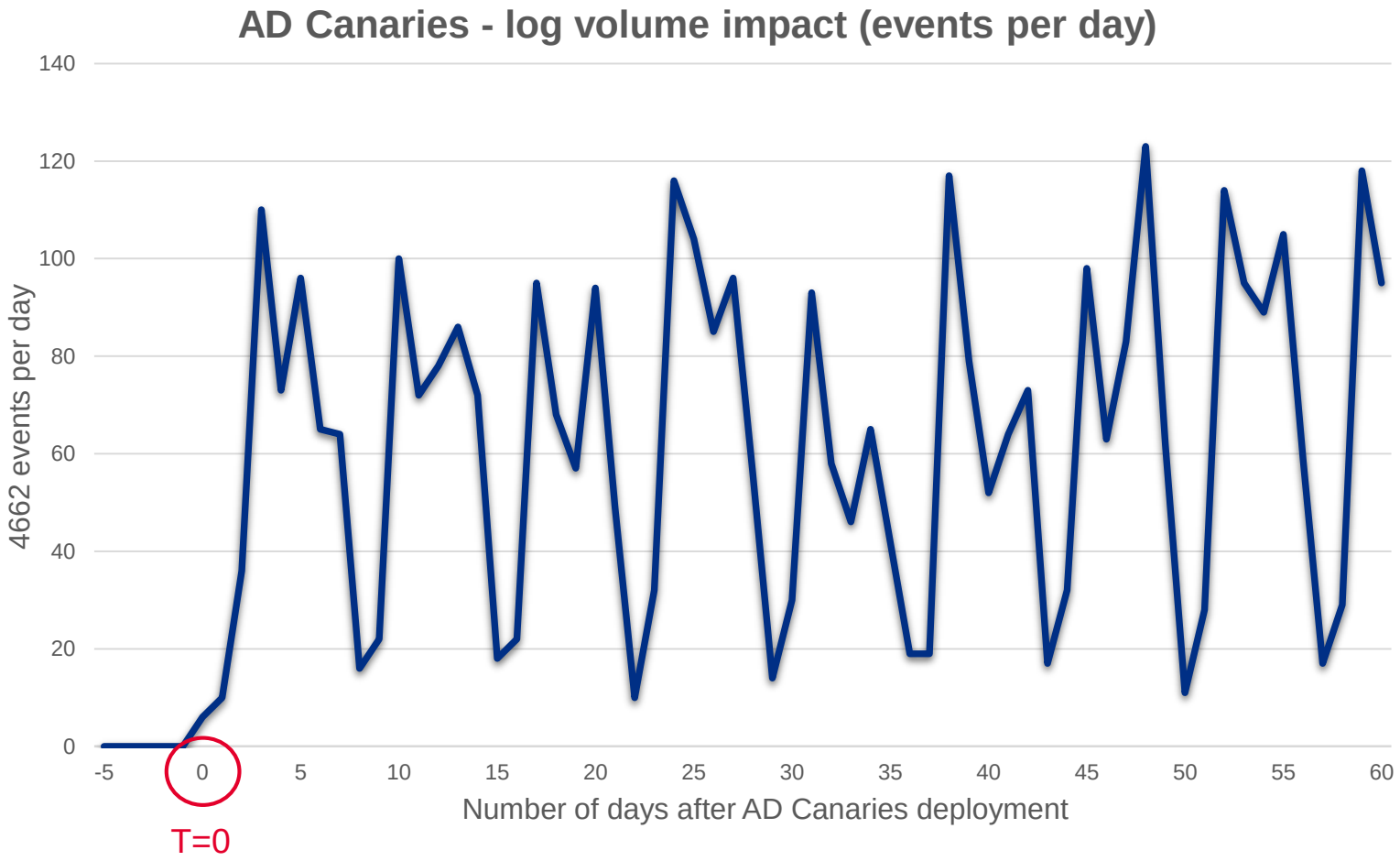
<u>60 jours après le déploiement:</u>

TUNING – 10j : ~15 exclusions
→ User + Propriétés accédées + Canari

PRE-RUN + RUN : ~8 incidents
(dont un test initié par le client)

Impact volumétrique : ~100 events/j

(contre 40 000 events/j précédemment sur un parc d'une taille inférieure!)



AIRBUS

AD Canaries : RETEX déploiement en production

Détecter, c'est bien. Qualifier, c'est mieux :

Qui a initié l'énumération ?

→ événement source : 4662

Qu'est ce qui a été énuméré ?

→ enrichissement lookups GUID

Depuis quel poste asset est initiée l'énumération ?

→ **pivot** événement Logon : 4624

Quel est le comportement à l'origine de l'énumération ?

→ **pivot** sur la télémétrie de l'asset identifié

→ Exécutions de processus

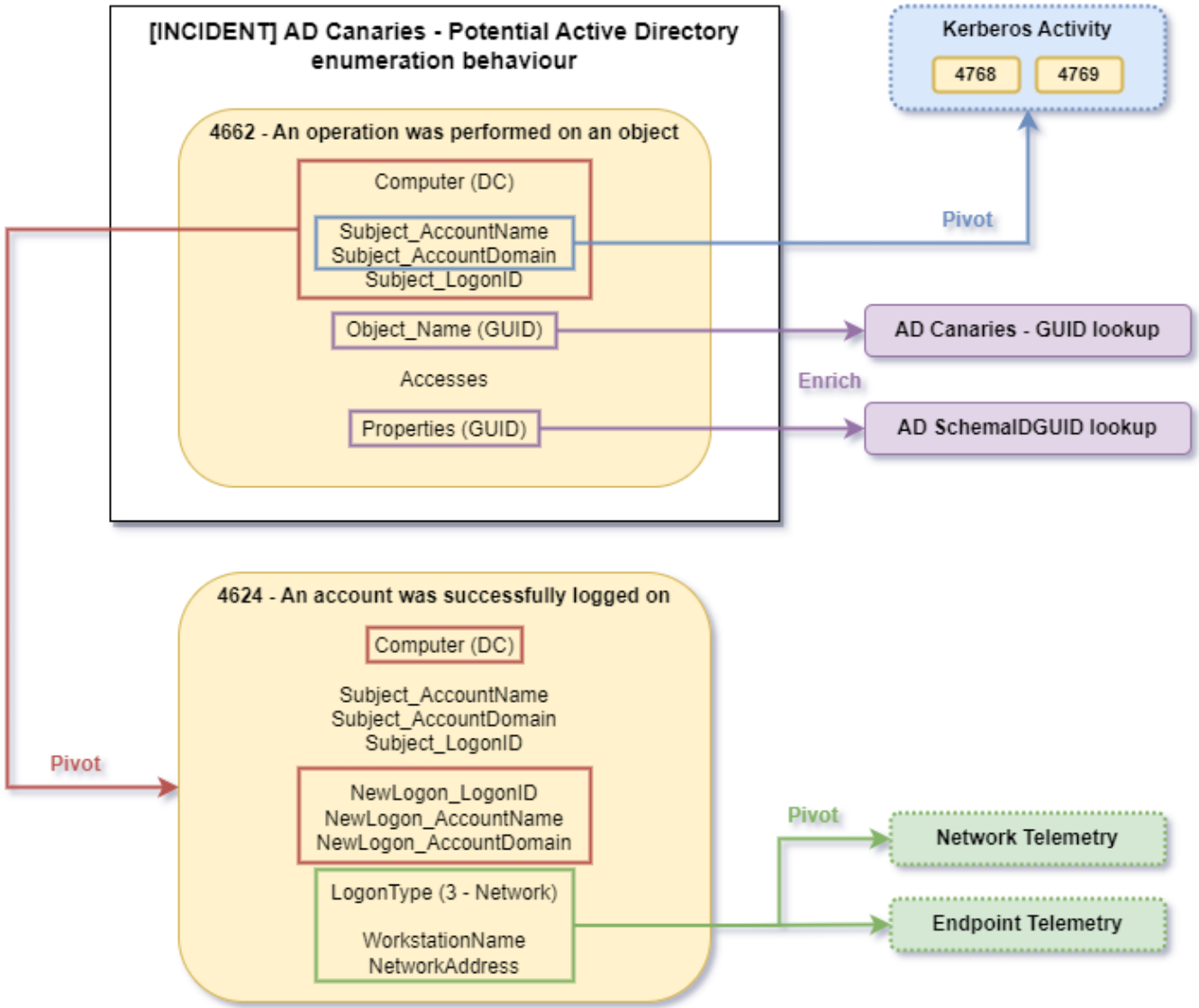
→ Connexions réseau

→ …

L'énumération coïncide-t-elle avec d'autres techniques d'attaques AD ?

→ **pivot** activité Kerberos du compte : 4768, 4769

→ **pivot** télémétrie réseau liée à l'asset identifié



AIRBUS

AD Canaries : RETEX déploiement en production

Echelle *subjective* des niveaux de difficultés / coûts associés au déploiement et au monitoring des canaris AD :

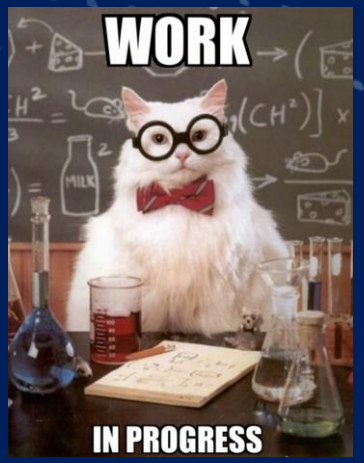
Task	Effort Level	Observations
Déploiement de la primitive de détection	1,5 / 5	• Objets isolés • Pas d'impact sur la surface d'attaque AD • Vérification politique audit / SACL • Equipe admin IT
Gestion des exclusions	2 / 5	• Très dépendant de l'environnement. • Identification des comportements relativement facile. • Nécessite un maintien des exclusions.
Impact sur la volumétrie	0 / 5	• La quantité d'événements générée est négligeable. • Pas de vérification du maintien des SACL.
Efforts d'investigations	3 / 5	• Dépends fortement de la télémétrie (endpoint, réseau) disponible. • Les pivots présentés permettent une qualification efficace dans la plupart des cas.
Alert fatigue	0 / 5	• Après tuning, la quantité d'incidents générés est extrêmement faible. • Maîtrise facile de la quantité d'incidents générés.

AIRBUS

Merci pour votre attention, des questions ?

Blog Airbus Protect: https://www.protect.airbus.com/insights/blog/

- 3 articles dédiés au sujet
- Publication du script de déploiement →



Twitter : @_Ar4h_

AIRBUS